COMMONWEALTH OFFICE OF TECHNOLOGY

COT Security Alert – Hackers Vow to Take Down Facebook

Hackers Vow To Take Down Facebook

Why you should be concerned…

Facebook has been listed as one of the recent targets for some of the members of the hacker collective, AntiSec. This group is infamous for distributing troves of compromised personal and confidential information from corporate, government and law enforcement databases.

How does this affect me?

Facebook is home of more than 750 million active users. It is important that users do not have the illusions of privacy when it comes to social networks. Users should assume that every single thing posted on the internet, is public record, forever. This is the nature of the beast.

Regardless if Facebook is compromised, please be cautious when using features like *"Login with Facebook",* and do not use the same password for your work and e-mail account. If your Facebook account is ever compromised or password exposed, this could give hackers access to dozens of affiliated sites and or systems that use the same credentials. It has been reported that even some banks have utilized Facebook's authentication technology to log in to their online banking sites.

5 Password Tips:

1. Do not use simple passwords: Social networks are havens for hacker reconnaissance. There are tools that can be ran against a profile, with the ability to generate a list of passwords to use based on the information that you share (names, hobbies, etc).

2. Do not use the same password: If you recycle your password and only one of the sites you visit (social networks, forums, banks) is compromised, it is only a matter of time before hackers will be able to gain access to other accounts. LulzSec is infamous for pasting the user credentials of compromised data - containing not only the typical citizen, but also government and military personnel; unfortunately, some of these users used the same password for their work e-mails as they did for whatever site was compromised.

With social networking and other internet accounts, there's plenty to offer hackers and by using the same password to access Facebook, Amazon and your online bank account, you're making it much easier for them.

3. Protect Your Password: Businesses expect you to use your password to stop others from misusing your account. If you share your password, you may be held responsible for what other people do with it.

4. Read Privacy Statements: Always read the privacy statement before you fill in the blanks. You should also verify that the site is using encryption before you submit any information — look for https in the web address and for a padlock or key in the lower right corner of your browser.

5. Password Complexity: If you can't remember difficult passwords no matter how hard you try, attempt to play around with it: ilovecoffee is a weak password; however, !1lov3Coffee! is much better. In addition creativity with your password, try to change your password often. A good security practice would be to change your password every 30 days.

Security Administration Branch
Commonwealth Office of Technology
120 Glenn's Creek Road, Jones Building
Frankfort, KY 40601
COTSecurityServicesISS@ky.gov
http://technology.ky.gov/CISO/